AMENDMENTS TO THE CLAIMS

Please replace all prior versions and listings of claims in the application with the listing of claims as follows:

Please amend claims 1, 21, 30, 39, and 56 as follows:

1. (Currently Amended) A processor-implemented method of detecting unauthorized access attempts to a network, comprising:

receiving a request from a user at a user address to obtain a target address;

obtaining said target address;

generating via a processor a substitute return address corresponding to output of a function applied to said target address and to said user address, said substitute return address corresponding to a used one of a block of substitute addresses;

returning said substitute return address to said user;

monitoring access to said target address; and

detecting an unauthorized attempt to access said target address when an attempted address corresponds to at least one unused substitute address of a group of unused substitute addresses in said block of substitute addresses, wherein said group of unused substitute addresses is user-specific.

2. (Previously Presented) The method according to claim 1, wherein said function further comprises hashing said user address of said user to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses and designating said group of unused substitute addresses by exclusion.

3. (Previously Amended) The method according to claim 2, wherein said function further comprises hashing a time of said request.

4. (Previously Amended) The method according to claim 2, wherein detecting comprises tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.

5. (Previously Amended) The method according to claim 4, comprising blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

6. (Previously Amended) The method according to claim 4, wherein unused ones of said block of substitute addresses correspond to attack detectors.

7. (Previously Amended) The method according to claim 1, wherein said function further comprises hashing a time of said request to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses.

8. (Previously Amended) The method according to claim 1, wherein said function further comprises changing said used one of said block of substitute addresses over time.

9. (Previously Amended) The method according to claim 8, wherein said function further comprises determining a time period for changing said one of said block of substitute addresses.

10. (Previously Presented) The method according to claim 9, wherein determining the time period comprises using a pre-selected time period.

11. (Previously Presented) The method according to claim 9, wherein determining the time period comprises generating a random time period.

12. (Previously Amended) The method according to claim 8, wherein changing said used one of said block of substitute addresses comprises randomly choosing said used one from said block of substitute addresses.

13. (Previously Amended) The method according to claim 8, wherein detecting comprises tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.

14. (Previously Amended) The method according to claim 13, comprising blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

15. (Previously Amended) The method according to claim 13, wherein unused ones of said block of substitute addresses correspond to attack detectors.

16. (Previously Amended) The method according to claim 8, further comprising determining said attempt is authorized when a connection exists between said user and said unused one of said block of substitute addresses.

17. (Previously Amended) The method according to claim 8, wherein changing said used one of said block of substitute addresses comprises coordinating changes in a name-to-address database and a host identity-to-address database.

18. (Previously Amended) The method according to claim 1, wherein detecting comprises tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.

19. (Previously Amended) The method according to claim 18, comprising blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

20. (Previously Amended) The method according to claim 1, wherein unused ones of said block of substitute addresses correspond to attack detectors.

21. (Currently Amended) A non-transitory computer-readable medium containing instructions for controlling a processor to detect unauthorized access attempts to a network by:

receiving a request from a user at a user address to obtain a target address;

obtaining said target address;

generating a substitute return address corresponding to output of a function applied to said target address, said substitute return address and to said user address corresponding to a used one of a block of substitute addresses;

returning said substitute return address to said user;

monitoring access to said target address; and

detecting an unauthorized attempt to access said target address when an attempted address corresponds to at least one unused substitute address of a group of unused substitute addresses in said block of substitute addresses, wherein said group of unused substitute addresses is user-specific.

22. (Previously Presented) The non-transitory computer-readable medium of claim 21, further comprising instructions for controlling the processor to apply said function by hashing a time of said request to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses.

23. (Previously Presented) The non-transitory computer-readable medium of claim 21, further comprising instructions for controlling the processor to detect said unauthorized attempt by tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.

24. (Previously Presented) The non-transitory computer-readable medium of claim 23, further comprising instructions for controlling the processor to detect said unauthorized attempt by blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

25. (Previously Presented) The non-transitory computer-readable medium of claim 21, further comprising instructions for controlling the processor to apply said function by changing said used one of said block of substitute addresses over time.

26. (Previously Presented) The non-transitory computer-readable medium of claim 25, further comprising instructions for controlling the processor to change said used one of said block of substitute addresses over time by at least one of determining a time period using a pre-selected time period and determining a time period by generating a random time period.

27. (Previously Presented) The non-transitory computer-readable medium of claim 25, further comprising instructions for controlling the processor to change said used one of said block of substitute addresses by randomly choosing said used one from said block of substitute addresses.

28. (Previously Presented) The non-transitory computer-readable medium of claim 25, further comprising instructions for controlling the processor to determine said attempt is authorized by determining that a connection exists between said user and said unused one of said block of substitute addresses.

29. (Previously Presented) The non-transitory computer-readable medium of claim 25, further comprising instructions for controlling the processor to change said used one of said block of substitute addresses by coordinating changes in a name-to-address database and a host identity-to-address database.

30. (Currently Amended) A system for detecting unauthorized access attempts to a network, comprising:

means for receiving a request from a user at a user address to obtain a target address;

means for obtaining said target address;

means for generating a substitute return address corresponding to output of a function applied to said target address, said substitute return address corresponding to a used one of a block of substitute addresses and to said user address, said means for generating including a processor programmed to apply said function to said target address and to said user address;

means for returning said substitute return address to said user;

means for monitoring access to said target address; and

means for detecting an unauthorized attempt to access said target address when an attempted address corresponds to at least one unused substitute address of a group of unused substitute addresses in said block of substitute addresses, wherein said group of unused substitute addresses is user-specific.

31. (Previously Presented) The system of claim 30, wherein said means for generating further comprises means for hashing a time of said request to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses.

32. (Previously Amended) The system of claim 30, wherein said means for detecting further comprise means for tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.

33. (Previously Amended) The system of claim 32, wherein said means for detecting further comprise means for blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

34. (Previously Amended) The system of claim 30, wherein said means for generating further comprise means for changing said used one of said block of substitute addresses over time.

35. (Original) The system of claim 34, wherein said means for changing further comprise at least one of means for determining a time period using a pre-selected time period and means for determining a time period by generating a random time period.

36. (Previously Amended) The system of claim 34, wherein said means for changing further comprise means for randomly choosing said used one from said block of substitute addresses.

37. (Previously Amended) The system of claim 34, further comprising means for determining said attempt is authorized when a connection exists between said user and said unused one of said block of substitute addresses.

38. (Original) The system of claim 34, further comprising:

a name-to-address database;

a host identity-to-address database; and means for coordinating changes in said name-to-address database and said host identity-to-address database in conjunction with said means for changing.

39. (Currently Amended) A computer program, disposed on a non-transitory computer-readable medium, for enabling detection of unauthorized access attempts to a network, said computer program including instructions for causing a processor to:

receive a request from a user at a user address to obtain a target address;

obtain said target address;

generate a substitute return address corresponding to output of a function applied to said target address and to said user address, said substitute return address corresponding to a used one of a block of substitute addresses;

return said substitute return address to said user;

monitor access to said target address; and

detect an unauthorized attempt to access said target address when an attempted address corresponds to at least one unused substitute address of a group of unused substitute addresses in said block of substitute addresses, wherein said group of unused substitute addresses is user-specific.

40. (Previously Presented) The computer program of claim 39, wherein said instructions for causing the processor to generate said substitute return address further include instructions for causing a processor to hash a time of said request to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses.

41. (Previously Amended) The computer program of claim 40, wherein said instructions for causing the processor to detect further include instructions for causing a processor to trace said user when said attempted address corresponds to said unused one of said block of substitute addresses.

42. (Previously Amended) The computer program of claim 41, further including instructions for causing the processor to block additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

43. (Previously Amended) The computer program of claim 41, further including instructions for causing the processor to correspond said unused ones of said block of substitute addresses with attack detectors.

44. (Previously Amended) The computer program of claim 39, wherein said instructions for causing the processor to generate said substitute return address further include instructions for causing a processor to change said used one of said block of substitute addresses over time.

45. (Previously Amended) The computer program of claim 44, wherein said instructions for causing the processor to generate said substitute return address further include instructions for causing a processor to at least one of use a pre-selected time period for changing said one of said block of substitute addresses and generate a random time period for changing said one of said block of substitute addresses.

46. (Previously Amended) The computer program of claim 44, wherein said instructions for causing the processor to change said used one of said block of substitute addresses further include instructions for causing a processor to randomly choose said used one from said block of substitute addresses.

47. (Previously Amended) The computer program of claim 44, wherein said instructions for causing the processor to detect further include instruction for causing a processor to trace said user when said attempted address corresponds to said unused one of said block of substitute addresses.

48. (Previously Amended) The computer program of claim 47, further including instructions for causing the processor to block additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

49. (Previously Amended) The computer program of claim 47, further including instructions for causing the processor to correspond attack detectors with unused ones of said block of substitute addresses.

50. (Previously Amended) The computer program of claim 44, further including instructions for causing the processor to determine said attempt is authorized when a connection exists between said user and said unused one of said block of substitute addresses.

51. (Previously Presented) The computer program of claim 44, further including instructions for causing the processor to coordinate said change in a name-to-address database and a host identity-to-address database.

52. (Previously Amended) The computer program of 39, wherein said instructions for causing the processor to detect further include instructions for causing a processor to trace said user when said attempted address corresponds to said unused one of said block of substitute addresses.

53. (Previously Amended) The computer program of claim 52, further including instructions for causing the processor to block additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

54. (Previously Amended) The computer program of claim 39, further including instructions for causing the processor to correspond attack detectors with unused ones of said block of substitute addresses.

55. (Previously Presented) The method of claim 1, wherein said group of unused substitute address is both user-specific and address-request-time-specific.

56. (Currently Amended) The method of claim 1, further comprising:

generating a new substitute return address for said target address after an expiration time has elapsed, wherein the expiration time is based on an expected session time for services associated with the address.